AUSA 10/29/14

14-2457 JMC
AUSA Harvey Eisenberg
410-209-4843

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

Special Agent Mark Gaskins, United States Secret Service, being duly sworn, states the following:

I. AFFIANT'S EXPERIENCE

I, Mark Gaskins, being duly sworn, declare and state:

1. I am a Special Agent of the United States Secret Service (USSS) and have been so employed since 1995. Currently, I am assigned to the Protection and Protective Intelligence Squad in the Baltimore Field Office of the USSS. I have received training in general law enforcement and criminal investigations, including protective intelligence investigations and have participated in numerous investigations related to crimes involving threats against the President and to his immediate family.

2. This affidavit is submitted for the limited purpose of establishing probable cause to believe that federal crimes have been committed by Christopher Perkins O'Brien and that evidence, fruits and instrumentalities of those crimes will be located at his residence, 2 Spa Creek Landing, Unit A3, Annapolis Maryland 21403. This affidavit is based upon my training and experience as well as information provided to me by other Special Agents of the USSS. Although I am not including all of the facts uncovered during the course of this investigation due to the limited purpose of this affidavit, I have not omitted any information that would tend to negate a finding of probable cause.

II. STATEMENT OF FACTS AND CIRCUMSTANCES

3. On October 16, 2014, the White House email comment site received an email from a person identifying himself as, "Mr. C.P. Obrien", with an alleged telephone number of [redacted] and a purported address of Boucher Avenue, Annapolis, Maryland. The captured IP address was recorded as 73.163.42.170. In the email, "Obrien" stated the following:

A.E.E. 10-29-14

"You stupid nigger, between ISIS, homegrown terrorists/beheaders here in the USA, and now your inaction on EBOLA, do you want us all to fucking die?!?! It sure as hell seems like that's what you want. You do not give a damn about protecting any of us from anything, do you?? I cannot wait to take out your worthless nigger ass, hope to reach out to slash Michele's throat, and crush your niglets wherever I find them on the grounds. You?? I will make a point to behead you, then throw your head into the nearest body of water, as I drive off into Maryland."

An inquiry for IP 73.163.42.170 resulted in its resolving to Comcast Cable in the Edgewater, Maryland area.

4. On October 18, 2014, USSS Special Agent Nathaniel Jones dialed the number provided in the email and a person answering the phone identified himself as Christopher O'Brien. Special Agent Jones informed O'Brien that his telephone number was provided in an email threat and was asked if he would agree to be interviewed. O'Brien agreed and provided his address as 2A3 Spa Creek Landing, Annapolis, Maryland. (This is simply another manner in which to describe the address of O'Brien). Upon arrival at that address later that day, Special Agent Jones, accompanied by USSS Special Agent Gary Eitel, introduced themselves to O'Brien and obtained his consent to both speak with the agents and to a search of his residence. O'Brien provided identification which showed his full true name to be Christopher Perkins O'Brien. During his time at the residence, Special Agent Jones observed a sheet of paper on the dining room table which had "IP 73.163.42.170" written on it among other writings.

5. During their conversation with O'Brien, the threatening email was read to him. At first O'Brien stated that he did not remember making the threat. In fact, he did so several times. After a time, however, O'Brien stated that he had, in fact, sent the email to the White House web site. He said that he had used the laptop computer at his

residence to send the email and that no one else had access to either his computer or his internet service. After admitting that he sent the threatening email, O'Brien stated that he never would harm the First Family and due to purported illnesses would not possess the means to carry out the threat. He also expressed regret in sending the email and stated that he was embarrassed.

6. Based upon the foregoing, it is my belief that there is probable cause to believe that Christopher Perkins O'Brien, on or about October 16, 2014, in the District of Maryland, did make a threat against the President of the United States in violation of 18 U.S.C. Section 871(a); did utilize interstate communications to make a threat to injure a person, specifically the President of the United States, in violation of 18 U.S.C. 875(c); and did make a threat to inflict bodily harm to the immediate family of the President of the United States in violation of 18 U.S.C 879(a)(2). Further, it is my belief that probable cause exists to believe that evidence, fruits and instrumentalities of those crimes are located at his residence, 2 Spa Creek Landing, Unit A3, Annapolis, Maryland 21403 as such items are more particularly described in Attachment B. In addition to the admission by O'Brien that he used the laptop computer located in his residence to commit the crimes specified herein, based upon my training and experience in investigating these types of crimes I know that persons committing these types of crimes customarily maintain documents that reflect research into their victims as well as research that would indicate their criminal state of mind. Additionally, their research also often doesn't result only in documents being created, but also results in an online trail that evidences their planning and/or criminal intent or which shows other, as yet unknown, similar threats.

III. SEIZURE AND SEARCH OF DIGITAL DEVICES

7. As used below, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central

processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes used to store digital data (excluding analog tapes such as VHS), and memory chips; and security devices. Based on my knowledge training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of the premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

8. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched.

9. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

10. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

11. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the

ACS 10/29/14

ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment.

12. Although some of the records called for by this warrant might be found in the form of user- generated documents (such as word processor, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment.

13. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not able to be separated from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment.

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises to be searched in whatever form they are found and that one form on which they may be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all pursuant to Rule 41(e)(2)(B).

WHEREFORE, it is respectfully requested that a search warrant be issued for the premises known as 2 Spa Creek Landing, Unit A3, Annapolis, Maryland 21403, more particularly described in Attachment A, and that such warrant authorize your affiant and other duly authorized law enforcement agents/officers to search said premises for items described

AES 10/23/14

in Attachment B and, if found, to seize said items pursuant to law and the procedures specified herein.

Special Agent Mark Gaskins
United States Secret Service

Subscribed and sworn to before me this day of October, 2014

J. Mark Coulson
United States Magistrate Judge

FILED ENTERED
LODGED RECEIVED

NOV 13 2014

AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND

BY DEPUTY

14-2457 JMC

~~14-2455 JMC~~